IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellant(s)	: Wankmueller *et al.*	Examiner	:	Firmin Backer
Serial No.	: 09/399,192	Confirmation No.	:	1972
Filed	: 09/17/1999	Group Art Unit	:	3621
For	: Apparatus And Method For Generating An Electronic-Commerce Personal Identification Number Cryptographically Related To An ATM Personal Identification Number			

AMENDED APPEAL BRIEF

Mail Stop Appeal
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST 3

II. RELATED APPEALS AND INTERFERENCES 4

III. STATUS OF CLAIMS 5

IV. STATUS OF AMENDMENTS 6

V. SUMMARY OF CLAIMED SUBJECT MATTER 7

VI. GROUNDS FOR REJECTION TO BE REVIEWED ON APPEAL 10

VII. ARGUMENT 11

VIII. CLAIMS APPENDIX 14

IX. EVIDENCE APPENDIX 25

X. RELATED PROCEEDINGS APPENDIX 26

I. REAL PARTY IN INTEREST

The real party in interest is MasterCard International Incorporated, 2000 Purchase Street, Purchase, New York 10577-2509 ("MasterCard"). MasterCard is the assignee of the entire right, title, and interest in the present application by virtue of an Assignment from John Wankmueller and Carl Campbell to MasterCard which was recorded on March 29, 1999 at Reel 009858, Frame 0707.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

III. STATUS OF CLAIMS

Claims 1-13, 17-29, 33-45, 49 and 50 stand rejected and claims 14-16, 30-32, and 46-48 are withdrawn.

Claims 1-13, 17-29, 33-45, 49 and 50 are the subject of this appeal. Appellants respectfully request review of all rejections of record.

IV. STATUS OF AMENDMENTS

Appellants have not submitted any amendments after filing of the Notice of Appeal.

V. SUMMARY OF CLAIMED SUBJECT MATTER

A. Independent Claim 1

1. A method for generating identification data [*See* Specification, p. 35, lns. 1-5], comprising the steps of:

providing an ATM PIN related to a first transaction type that is an ATM transaction [*See* Specification, p. 3, ln. 17 - p. 4, ln 2]; and

generating a non-ATM electronic commerce PIN on a central computer by performing a cryptographic operation on said ATM PIN [*See* Specification, p. 4, lns. 3-5], said non-ATM electronic commerce PIN to be entered by a user in a second transaction type that is a non-ATM financial transaction [*See* Specification, p. 3, ln. 17 - p. 4, ln 2]; and

transmitting said non-ATM electronic commerce PIN to said user [*See* Specification, p. 12, lns. 19-20].

B. Independent Claim 17

17. A system for generating identification data [*See* Specification, p. 35, lns. 1-5], comprising:

a memory for storing an ATM PIN [*See* Specification, p. 13, lns. 1-5];

a processor on a central computer for performing a cryptographic operation upon the ATM PIN [*See* Specification, p. 7, lns. 10-16], such that said processor generates a second non-ATM PIN related to a non-ATM electronic transaction during which transaction a user enters said second non-ATM PIN [*See* Specification, p. 3, ln. 17 - p. 4, ln 2]; and

a transmission means for transmitting said non-ATM PIN to said user [*See* Specification, p. 12, lns. 19-20].

C. Independent Claim 33

33. A system for generating identification data [*See* Specification, p. 35, lns. 1-5], comprising:

a memory on a central computer [*See* Specification, p. 13, lns. 1-5];

a processor on said central computer in communication with the memory [*See* Specification, p. 7, lns. 10-16];

a computer-readable medium on said central computer in communication with the processor and storing instructions which, when executed, cause the processor to perform the steps of:

storing an ATM PIN in the memory, said first set being related to a first transaction type [*See* Specification, p. 10, lns. 18-19; FIG. 1, Step 301];

performing a cryptographic operation upon the ATM PIN, thereby generating a second PIN to be entered by a user during a non-ATM electronic transaction [*See* Specification, p. 4, lns. 3-5]; and

means for transmitting said non-ATM PIN to said user [*See* Specification, p. 12, lns. 19-20].

D. Independent Claim 49

49. A method for generating identification data for a non-ATM electronic financial transaction over a communications network [*See* Specification, p. 35, lns. 1-5], comprising the steps of:

providing a first set of identification data related to a first transaction type [*See* Specification, p. 10, lns. 18-19; p. 13, lns. 2-5; FIG. 1, Step 301;];

generating a second set of identification data on a central computer by performing a cryptographic operation on said first set of identification data [*See* Specification, p. 4, lns. 3-5], wherein said first set of identification data is an ATM PIN, said first transaction type is an ATM-transaction, said second set of identification data is a non-ATM electronic commerce PIN to be entered by a user in a non-ATM electronic financial transaction [*See* Specification, p. 6, lns. 2-11]; and

transmitting said non-ATM electronic commerce PIN to said user [*See* Specification, p. 12, lns. 19-20].

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection for review are:

(1) Rejection of claims 1-13, 17-29, 33-45, 49 and 50 under 35 U.S.C. § 102(b) as being anticipated by Khello U.S. Patent No. 5,724,423 (hereinafter "Khello").

Appellants respectfully traverse the rejection of claims 1-13, 17-29, 33-45, 49 and 50.

VII. ARGUMENT

In the Office Action dated October 10, 2006, claims 1-13, 17-29, 33-45, 49 and 50 were rejected under 35 U.S.C. § 102(b) as allegedly anticipated by Khello.

A. Summary of Khello

Khello is directed to a portable apparatus for user authentication. A user of Khello's system may enter a personal identification number ("PIN") and a positive integer using a portable terminal device (*See* Abstract; Fig. 2). The portable terminal device encrypts the PIN and combines it with a random code before transmitting it over a communications network (*See* Abstract; Fig. 5(a)). When received, the encoded PIN is decoded to determine if the user is authorized (*See* Figs. 5(a) and 5(b); Col. 14, ln. 56 - Col. 15, ln. 3).

B. Rejection of claims 1-13, 17-29, 33-45, 49 and 50 as anticipated by Khello

The Examiner has rejected independent claim 1 as being anticipated by Khello (*See* October 10, 2006 Office Action, p. 2). The Examiner has also rejected independent claims 17, 33, and 49 using "similar rationale" (*See* October 10, 2006 Office Action, p. 4). Therefore, Appellants believe that the arguments presented below with respect to claim 1 should also be applied to independent claims 17, 33, and 49 and all claims dependent thereupon.

With respect to claim 1, the Examiner alleges that Khello discloses a method for generating identification data comprising providing an ATM PIN (*pin*) related to a first transaction type; and generating a non ATM electronic commerce PIN (*random code*) on a central computer by performing a cryptographic operation on the ATM PIN for second transaction which is a non ATM transaction to be entered by a user in a second transaction type that is a non-ATM transaction (*See* October 10, 2006 Office Action, p. 2, *citing* Khello, Abstract; Col. 2 - Col. 3, ln. 35).

First, the Examiner has not stated that Khello discloses the claim limitation of "transmitting said non-ATM electronic commerce PIN to said user" as recited in claim 1 (and in independent claims 17, 33, and 49). Appellants submit that this step would not be possible utilizing the system of Khello because the "random code," which the Examiner has likened to the non ATM electronic commerce PIN, is only utilized to encrypt the PIN entered by the user and is never transmitted to the user. In fact, Khello teaches away from transmitting a second PIN to the user stating "**it is an object of the present invention to provide a high level of security that only requires a user to memorize *one PIN code***" (*See* Khello, Col. 2, lns. 43-45 (emphasis added)). Additionally, the entire background section of Khello discusses in general terms this same point (*See* Col. 1, ln. 11 - Col. 2, ln. 33).

In addition, the two codes generated in Khello are utilized in the same transaction (and therefore inherently the same "transaction type"), whereas claim 1 (and independent claims 17, 33, and 49) requires the user to enter the non-ATM electronic commerce PIN in a "second transaction type" and, accordingly, not the same transaction type.

Further, Appellants submit that Khello does not disclose the claim limitation of "generating a non-ATM electronic commerce PIN on a central computer." In Khello, for each and every transaction, the portable terminal device dynamically generates an encrypted, randomized PIN that is different for each transaction. The user does not have to remember the generated PIN (indeed, as a practical matter, the user cannot, since a new PIN is generated for every transaction in Khello), nor does the user ever have to enter this generated PIN to complete a transaction (*See* Khello Abstract; Fig. 2; Col. 3, lns. 12-35). In the claimed invention, on the other hand, not only does the *central computer* generate the non-ATM electronic commerce PIN,

the non-ATM electronic commerce PIN generated by the central computer is intended to be memorized by the user and used **multiple times** in **more than one type of transaction**.

For the aforementioned reasons and arguments, Appellants respectfully requests that the rejection of independent claims 1, 17, 33 and 49 and all claims depending thereon should be withdrawn.

VIII. CLAIMS APPENDIX

1. A method for generating identification data, comprising the steps of:

providing an ATM PIN related to a first transaction type that is an ATM transaction; and

generating a non-ATM electronic commerce PIN on a central computer by performing a cryptographic operation on said ATM PIN, said non-ATM electronic commerce PIN to be entered by a user in a second transaction type that is a non-ATM financial transaction; and

transmitting said non-ATM electronic commerce PIN to said user.

2. A method according to claim 1, wherein the step of performing a cryptographic operation comprises:

providing a conversion key; and

using the conversion key to perform said cryptographic operation upon the ATM PIN.

3. A method according to claim 2, wherein the step of providing a conversion key comprises:

providing conversion key derivation data;

providing a conversion key derivation key; and

performing a cryptographic operation upon the conversion key derivation data and the conversion key derivation key.

4. A method according to claim 3, wherein the step of performing a cryptographic operation upon the conversion key derivation data and the conversion key derivation key

comprises using the conversion key derivation key to perform at least one cryptographic operation upon the conversion key derivation data.

5. A method according to claim 4, wherein the conversion key derivation data includes an identification number that is associated with multiple accounts, and wherein at least one cryptographic operation using a secret key is performed to cryptographically process said conversion key derivation data to produce the conversion key.

6. A method according to claim 1, wherein the step of performing a cryptographic operation comprises:

providing cryptographically-computed data; and

performing an operation upon the ATM PIN and the cryptographically-computed data.

7. A method according to claim 6, wherein the step of providing cryptographically-computed data comprises:

providing initial data; and

performing at least one cryptographic operation using a secret key upon the initial data, thereby producing the cryptographically-computed data.

8. A method according to claim 7, wherein said at least one cryptographic operation using a secret key comprises at least one of a DES-encryption and a DES-decryption.

9. A method according to claim 8, wherein at least a portion of the initial data is obtained from at least a portion of an account number.

10. A method according to claim 9, wherein the operation upon the ATM PIN and the cryptographically-computed data comprises either a subtraction operation or an addition operation.

11. A method according to claim 10, wherein the step of providing cryptographically-computed data further comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the ATM PIN.

12. A method according to claim 6, wherein the step of providing cryptographically-computed data comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the ATM PIN.

13. A method according to claim 6, wherein the operation upon the ATM PIN and the cryptographically-computed data comprises either a subtraction operation or an addition operation.

17. A system for generating identification data, comprising:

a memory for storing an ATM PIN;

a processor on a central computer for performing a cryptographic operation upon the ATM PIN, such that said processor generates a second non-ATM PIN related to a non-ATM electronic transaction during which transaction a user enters said second non-ATM PIN; and

a transmission means for transmitting said non-ATM PIN to said user.

18. The system of claim 17, wherein the memory includes means for storing a conversion key, and wherein the processor comprises means for using the conversion key to perform a cryptographic operation upon the ATM PIN.

19. The system of claim 18, wherein the memory further includes:

means for storing conversion key derivation data; and

means for storing a conversion key derivation key; and

wherein the processor comprises means to perform a cryptographic operation upon the conversion key derivation data and the conversion key derivation key, thereby generating the conversion key.

20. The system of claim 19, wherein the cryptographic operation upon the conversion key derivation data and the conversion key derivation key comprises at least one DES operation.

21. The system of claim 20, wherein the conversion key derivation data is derived from an identification number, and wherein said at least one DES operation comprises:

using a portion of the conversion key derivation key to DES-encrypt the conversion key derivation data, thereby producing a first conversion key generation result;

using a portion of the conversion key derivation key to DES-decrypt the first conversion key generation result, thereby producing a second conversion key generation result;

using a portion of the conversion key derivation key to DES-encrypt the second conversion key generation result, thereby producing a third conversion key generation result;

using the third conversion key generation result as a first portion of the conversion key;

using a portion of the conversion key derivation key to DES-encrypt the third conversion key generation result, thereby producing a fourth conversion key generation result;

using a portion of the conversion key derivation key to DES-decrypt the fourth conversion key generation result, thereby producing a fifth conversion key generation result;

using a portion of the conversion key derivation key to DES-encrypt the fifth conversion key generation result, thereby producing a sixth conversion key generation result; and

using the sixth conversion key generation result as a second portion of the conversion key.

22. The system of claim 17, wherein the memory includes means for storing cryptographically-computed data, and wherein the processor comprises:

means for generating the cryptographically-computed data; and

means for performing an operation upon the ATM PIN and the cryptographically-computed data.

23. The system of claim 22, wherein the memory further includes means for storing initial data, and wherein the means for generating the cryptographically-computed data comprises means for performing at least one cryptographic operation upon the initial data, thereby producing the cryptographically-computed data.

24. The system of claim 23, wherein said at least one cryptographic operation comprises at least one of a DES-encryption and a DES-decryption.

25. The system of claim 24, wherein the initial data is obtained from an account number, wherein the memory further includes means for storing a conversion key, and wherein the cryptographic operation uses the initial data and the conversion key to produce the cryptographically-computed data.

26. The system of claim 25, wherein the means for performing an operation upon the ATM PIN and the cryptographically-computed data comprises either a subtraction means or an addition means.

27. The system of claim 25, wherein the means for performing an operation further comprises means for generating a cryptographically-computed number having a base corresponding to a base of a number representing the ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the ATM PIN.

28. The system of claim 22, wherein the means for performing an operation comprises means for generating a cryptographically-computed number having a base corresponding to a base of a number representing ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the ATM PIN.

29. The system of claim 22, wherein the means for performing an operation comprises either a subtraction means or an addition means.

33. A system for generating identification data, comprising:

a memory on a central computer;

a processor on said central computer in communication with the memory;

a computer-readable medium on said central computer in communication with the processor and storing instructions which, when executed, cause the processor to perform the steps of:

storing an ATM PIN in the memory, said first set being related to a first transaction type;

performing a cryptographic operation upon the ATM PIN, thereby generating a second PIN to be entered by a user during a non-ATM electronic transaction; and

means for transmitting said non-ATM PIN to said user.

34. The system of claim 33, wherein the step of performing a cryptographic operation comprises:

providing a conversion key;

storing the conversion key in the memory; and

using the conversion key to perform said cryptographic operation upon the ATM PIN.

35. The system of claim 34, wherein the step of providing a conversion key comprises:

storing conversion key derivation data in the memory;

storing a conversion key derivation key in the memory; and

performing a cryptographic operation upon the conversion key derivation data and the conversion key derivation key.

36. The system of claim 35, wherein the step of performing a cryptographic operation upon the conversion key derivation data and the conversion key derivation key comprises using the conversion key derivation key to perform at least one DES operation upon the conversion key derivation data.

37. The system of claim 36, wherein the conversion key derivation data is derived from an identification number, and wherein said at least one DES operation comprises:

using a portion of the conversion key derivation key to DES-encrypt the conversion key derivation data, thereby producing a first conversion key generation result;

using a portion of the conversion key derivation key to DES-decrypt the first conversion key generation result, thereby producing a second conversion key generation result;

using a portion of the conversion key derivation key to DES-encrypt the second conversion key generation result, thereby producing a third conversion key generation result;

using the third conversion key generation result as a first portion of the conversion key;

using a portion of the conversion key derivation key to DES-encrypt the third conversion key generation result, thereby producing a fourth conversion key generation result;

using a portion of the conversion key derivation key to DES-decrypt the fourth conversion key generation result, thereby producing a fifth conversion key generation result;

using a portion of the conversion key derivation key to DES-encrypt the fifth conversion key generation result, thereby producing a sixth conversion key generation result; and

using the sixth conversion key generation result as a second portion of the conversion key.

38. The system of claim 33, wherein the step of performing a cryptographic operation comprises:

providing cryptographically-computed data;

storing the cryptographically-computed data in the memory; and

performing an operation upon the ATM PIN and the cryptographically-computed data.

39. The system of claim 38, wherein the step of providing cryptographically-computed data comprises:

storing initial data in the memory; and

performing at least one cryptographic operation using a secret key upon the initial data, thereby producing the cryptographically-computed data.

40. The system of claim 39, wherein said at least one cryptographic operation using a secret key comprises at least one of a DES-encryption and a DES-decryption.

41. The system of claim 40, wherein at least a portion of the initial data is obtained from at least a portion of an account number.

42. The system of claim 41, wherein the operation upon the ATM PIN and the cryptographically-computed data comprises either a subtraction operation or an addition operation.

43. The system of claim 42, wherein the step of providing cryptographically-computed data further comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the ATM PIN.

44. The system of claim 38, wherein the step of providing cryptographically-computed data comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the ATM PIN, wherein said